DIN EN ISO 25237:2017-05 (E)

Health informatics - Pseudonymization (ISO 25237:2017)

Contents

Page

European foreword **4**

Foreword **5**

Introduction **6**

1 Scope **7**

2 Normative references **7**

3 Terms and definitions **7**

4 Abbreviated terms **12**

5 Requirements for privacy protection of identities in healthcare **13**

5.1 Objectives of privacy protection 13
5.2 General 13
5.3 De-identification as a process to reduce risk 14
5.3.1 General 14
5.3.2 Pseudonymization 14
5.3.3 Anonymization 15
5.3.4 Direct and indirect identifiers 15
5.4 Privacy protection of entities 15
5.4.1 Personal data versus de-identified data 15
5.4.2 Concept of pseudonymization 17
5.5 Real world pseudonymization 19
5.5.1 Rationale 19
5.5.2 Levels of assurance of privacy protection 20
5.6 Categories of data subject 22
5.6.1 General 22
5.6.2 Subject of care 22
5.6.3 Health professionals and organizations 22
5.6.4 Device data 22
5.7 Classification data 23
5.7.1 Payload data 23
5.7.2 Observational data 23
5.7.3 Pseudonymized data 23
5.7.4 Anonymized data 23
5.8 Research data 23
5.8.1 General 23
5.8.2 Generation of research data 24
5.8.3 Secondary use of personal health information 24
5.9 Identifying data 24
5.9.1 General 24
5.9.2 Healthcare identifiers 24
5.10 Data of victims of violence and publicly known persons 25
5.10.1 General 25
5.10.2 Genetic information 25
5.10.3 Trusted service 25
5.10.4 Need for re-identification of pseudonymized data 25
5.10.5 Pseudonymization service characteristics 26

6 Protecting privacy through pseudonymization **26**
6.1 Conceptual model of the problem areas 26
6.2 Direct and indirect identifiability of personal information 27
6.2.1 General 27
6.2.2 Person identifying variables 27
6.2.3 Aggregation variables 27
6.2.4 Outlier variables 28
6.2.5 Structured data variables 28
6.2.6 Non-structured data variables 29
6.2.7 Inference risk assessment 29
6.2.8 Privacy and security 30

7 Re-identification process **30**
7.1 General 30
7.2 Part of normal procedures 30
7.3 Exception 30
7.4 Technical feasibility 31

Annex A (informative) **Healthcare pseudonymization scenarios** **32**

Annex B (informative) **Requirements for privacy risk analysis** **45**

Annex C (informative) **Pseudonymization process (methods and implementation)** **55**

Annex D (informative) **Specification of methods and implementation** **61**

Annex E (informative) **Policy framework for operation of pseudonymization services (methods and implementation)** **62**

Annex F (informative) **Genetic information** **65**

Bibliography **66**